ABSTRACT OF THE DISCLOSURE

1
2
3   A page fault proxy handler and related method defend against buffer overflow attacks.

4   The page fault proxy handler is for connection to an original page fault handler and a paging

5   table in which supervisor flags for all entries for all writable memory pages have been pre-set.

6   The page fault proxy handler comprises a page fault detector, a page fault filter, an execution

7   address checker, a mitigation module, and a controlled memory access module. The detector

8   detects page faults and passes them to the filter. The filter passes to the original page fault

9   handler page faults not arising from an attempt to access a writable page by a user mode

10   program. The execution address checker passes to the mitigation module only page faults

11   arising from an attempt by a user mode program to execute from the writable page; other

12   accesses to a writable page by a user mode program are passed to the controlled memory

13   access module. The mitigation logs and/or terminates the program. The controlled memory

14   access module permits the user program to access the writable page by changing an associated

15   supervisor flag in the paging table. The method handles page faults in conjunction with an

16   original page fault handler. The method sets a supervisor flag in a page entry table associated

17   with a writable page. The method detects a page fault and determines whether it arises from

18   an attempt by a user mode program to execute from the writable page having the associated

19   supervisor flag set. The method conditionally calls the original page fault handler on the

20   basis of the determining step.